



FortiAuthenticator™ Certificate Based SSL VPN

Solution Guide



FortiAuthenticator™ Certificate Based SSL VPN Solution Guide

October 23, 2013

Revision 1

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation

<http://help.fortinet.com>

Knowledge Base

<http://kb.fortinet.com>

Forums

<https://support.fortinet.com/forums>

Customer Service & Support

<https://support.fortinet.com>

Training

<http://training.fortinet.com>

FortiGuard Threat Research & Response

<http://www.fortiguard.com>

License Agreement

<http://www.fortinet.com/doc/legal/EULA.pdf>

Document Feedback

Email: techdocs@fortinet.com

Table of contents

Change Log	4
Introduction.....	5
Software Versions.....	5
FortiAuthenticator Certificate Based SSL VPN Guide.....	6
Introduction	6
Topology.....	6
FortiAuthenticator Root Certificate	6
FortiAuthenticator User Certificate.....	8
FortiAuthenticator Directory Services Configuration	13
FortiGate Certificate Configuration	14
FortiGate RADIUS Client Configuration	15
FortiGate SSL-VPN Configuration.....	16
Testing, Logging and Monitoring	19
Additional Considerations - Certificate Checking.....	23
Added Benefits	23

Change Log

Revision	Date	Change Description
1	2013-10-23	Initial revision

Introduction

This document provides a configuration guide for setting up certificate based SSL-VPNs using FortiGate and FortiAuthenticator. The guide provides a step by step walkthrough on both the FortiAuthenticator and the FortiGate, however, for a detailed understanding on PKI and certificate authentication further reading is required, as the objective of this guide is to provide a configuration walkthrough.

Software Versions

The configuration discussed in this document was tested on the following firmware versions:

- FortiAuthenticator 3.0
- FortiOS 5.0 GA Patch Release 4

FortiAuthenticator Certificate Based SSL VPN Guide

Introduction

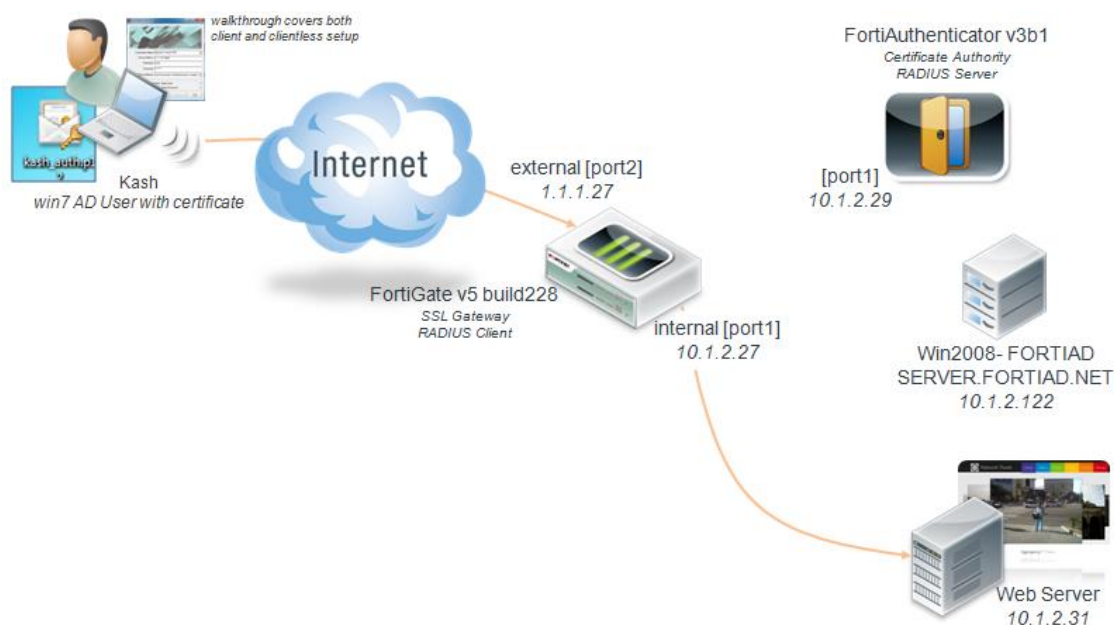
The purpose of this document is to provide a configuration guide on how to setup certificate based SSL-VPNs, using FortiGate and FortiAuthenticator. The guide covers various subject areas such as PKI and VPNs, further reading is required for a detailed understanding on the theory of such topics, the intention of this document is to provide a concise configuration guide which will allow for the successful configuration of certificate based VPNs.

The guide will step through the FortiAuthenticator configuration before moving on to the FortiGate, before testing the setup. All the topology components are using factory default settings, except for the IP configuration.



Note: Before commencing the configuration, please ensure that the date and time are correctly configured and synchronized across all of the topology elements.

Topology



FortiAuthenticator Root Certificate

To commence the certificate setup on the FortiAuthenticator, a Certificate Authority root certificate has to be created (the FortiAuthenticator is the Certificate Authority in this configuration).

Under *Certificate Management* > *Certificate Authorities* > *Local CAs* Click **Create New**
Complete the relevant certificate, example below and **OK** the changes.

Create New Local CA Certificate

Certificate ID:

Certificate Authority Type

Certificate type:

☒ Root CA certificate
 ☐ Intermediate CA certificate
 ☐ Intermediate CA certificate signing request (CSR)

Subject Information

Subject input method:

☐ Fully distinguished name
 ☒ Field-by-field

Name (CN):

Department (OU):

Company (O):

City (L):

State/Province (ST):

Country (C):

E-mail address:

Subject Alternative Name

☐ Email:

☐ User Principal Name (UPN):

Additional Options

Validity period:

☒ Set length of time
 ☐ Set an expiry date

days

Key type:

Key size:

Hash algorithm:

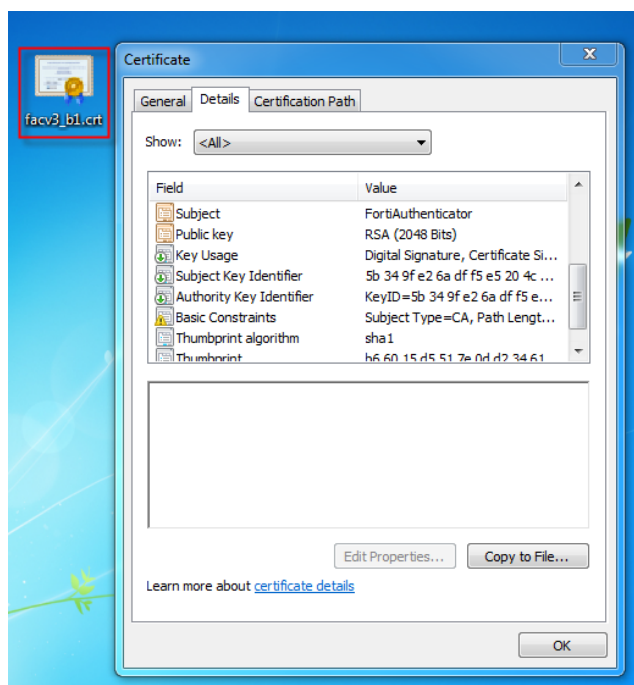
OK

Cancel

Once the certificate has been created, select the certificate and then click on **Export**.

✔ Successfully added local CA certificate "facy3_b1 CN=FortiAuthenticator".					
<input checked="" type="checkbox"/>	Certificate ID	Subject	Issuer	Status	CA Type
<input checked="" type="checkbox"/>	facy3_b1	CN=FortiAuthenticator	CN=FortiAuthenticator	Active	Root CA

Save the certificate to the desktop (or appropriate folder). Once the certificate is saved, it should be possible to **double click** on the certificate to view the details, see below.



FortiAuthenticator User Certificate

The next certificate based task is to create the user certificate. Within the FortiAuthenticator interface, go to *Certificate Management > End Entities > Users* and click on **Create New**. Then complete the relevant user certificate fields and click on **OK**, example below.

Create New User Certificate	
Certificate ID:	kash_auth
Certificate Signing Options	
Issuer:	<input checked="" type="radio"/> Local CA <input type="radio"/> Third-party CA
Local User (Optional):	[Please Select]
Certificate authority:	facv3_b1 CN=FortiAuthenticator
Subject Information	
Subject input method:	<input type="radio"/> Fully distinguished name <input checked="" type="radio"/> Field-by-field
Name (CN):	kash
Department (OU):	system engineering
Company (O):	fortinet
City (L):	london
State/Province (ST):	
Country (C):	Britain (UK) (GB)
E-mail address:	kash@fortinet.com

Subject Alternative Name

☐ Email:

☐ User Principal Name (UPN):

Additional Options

Validity period: ☒ Set length of time ☐ Set an expiry date

days

Key type: RSA

Key size: Bits

Hash algorithm:

Other Extensions

☐ Add CRL Distribution Points extension (Location: DNS domain name has not been configured) [Edit DNS name]

☐ Use certificate for Smart Card logon

OK Cancel

Once the certificate has been completed and **OK**'d, then export the certificate with the private key by selecting the certificate and clicking on **Export PKCS#12** button.

Create New Import Revoke Delete Export Certificate **Export PKCS#12** 1 of 1 selected Search for user certificates Search

Successfully added user certificate "kash_auth | C=GB, L=london, O=fortinet, OU=system engineering, CN=kash, emailAddress=kash@fortinet.com".

<input checked="" type="checkbox"/>	Certificate ID	Subject	Issuer	Status
<input checked="" type="checkbox"/>	kash_auth	C=GB, L=london, O=fortinet, OU=system engineering, CN=kash, e...	CN=FortiAuthenticator	Active

Add a *passphrase* to the certificate being exported and click **OK**.

Export User Certificate and Key File

Subject: C=GB, L=london, O=fortinet, OU=system engineering, CN=kash, emailAddress=kash@fortinet.com

Passphrase:

Confirm Passphrase:

OK Cancel

Then download the file to the desktop (or appropriate folder) by *clicking Finish*.

Download PKCS#12 Certificate File

Please note that once you click on the download link below, the private key for certificate "C=GB, L=london, O=fortinet, OU=system engineering, CN=kash, emailAddress=kash@fortinet.com" will be removed.

[Download PKCS#12 file](#)

Click **Finish** to return to the certificate list.

Finish

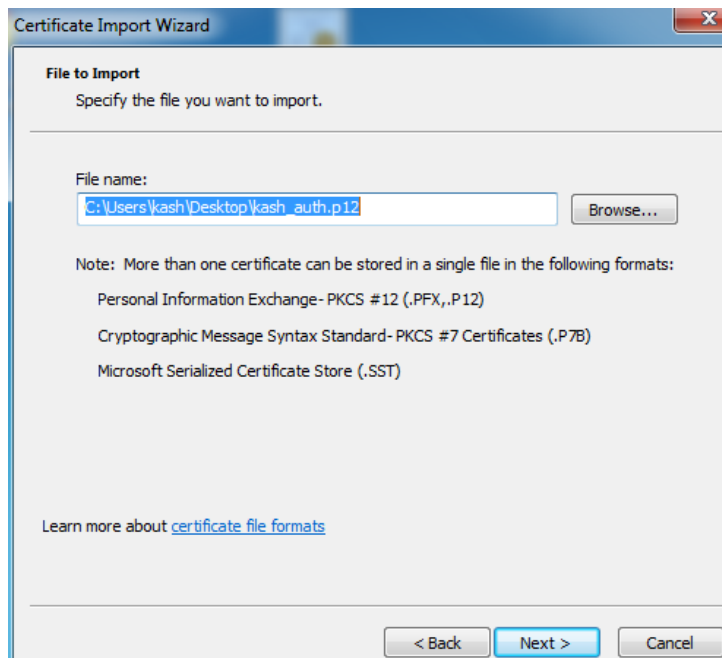
The **PKCS12#** file should be in the following format on the desktop



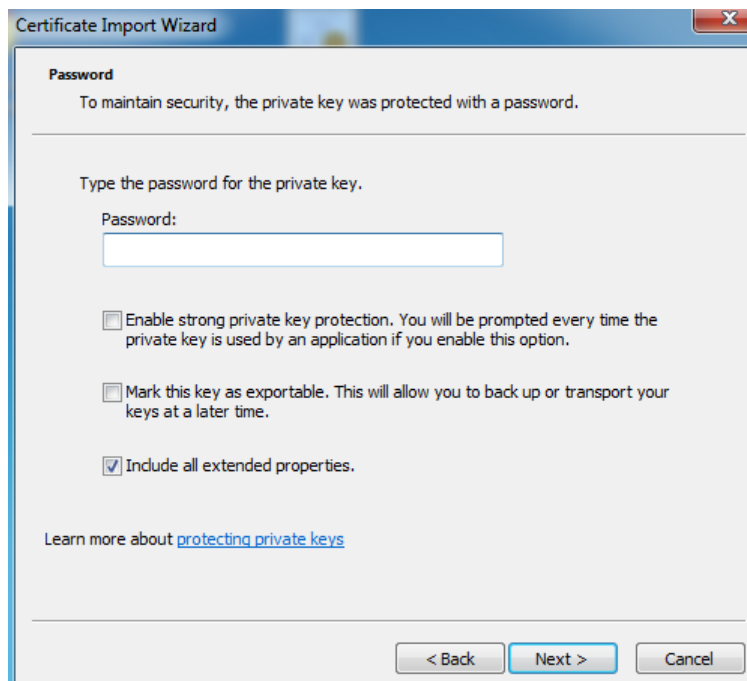
Double Click the PKCS12# file, this should then start an automatic import wizard, see below, on Welcome screen, click **Next**



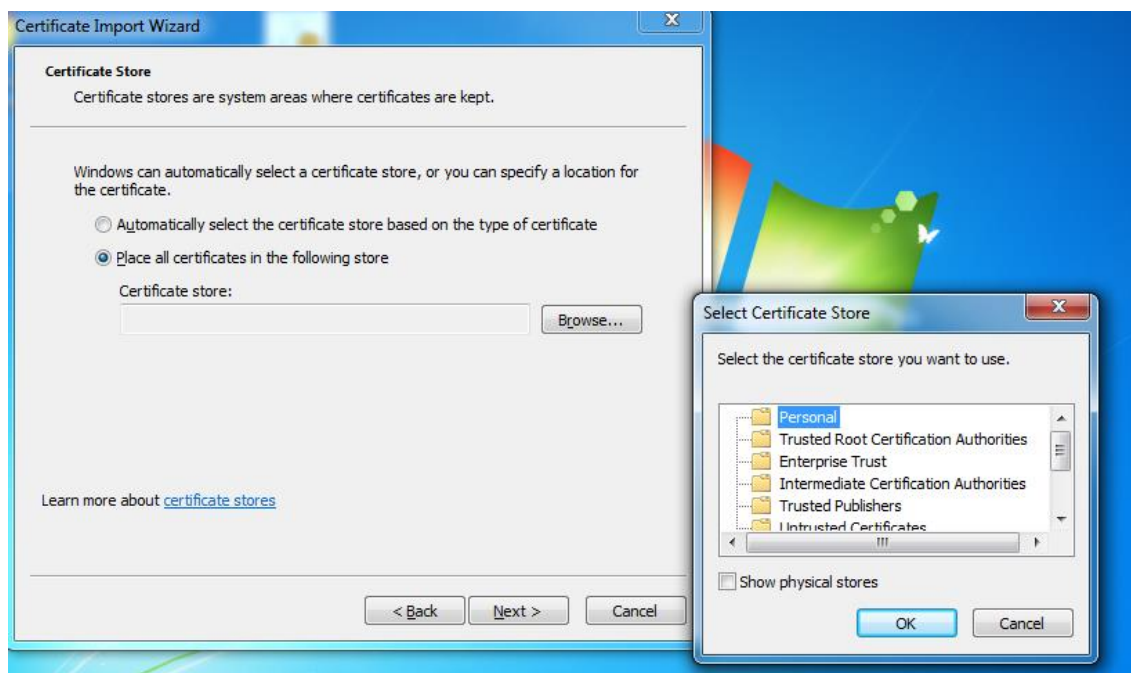
Ensure that the correct **PKCS12#** file is selected and click **Next**.



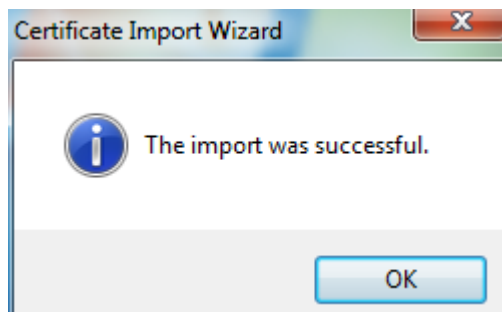
Enter the passphrase used during the export from the FortiAuthenticator and click **Next**.



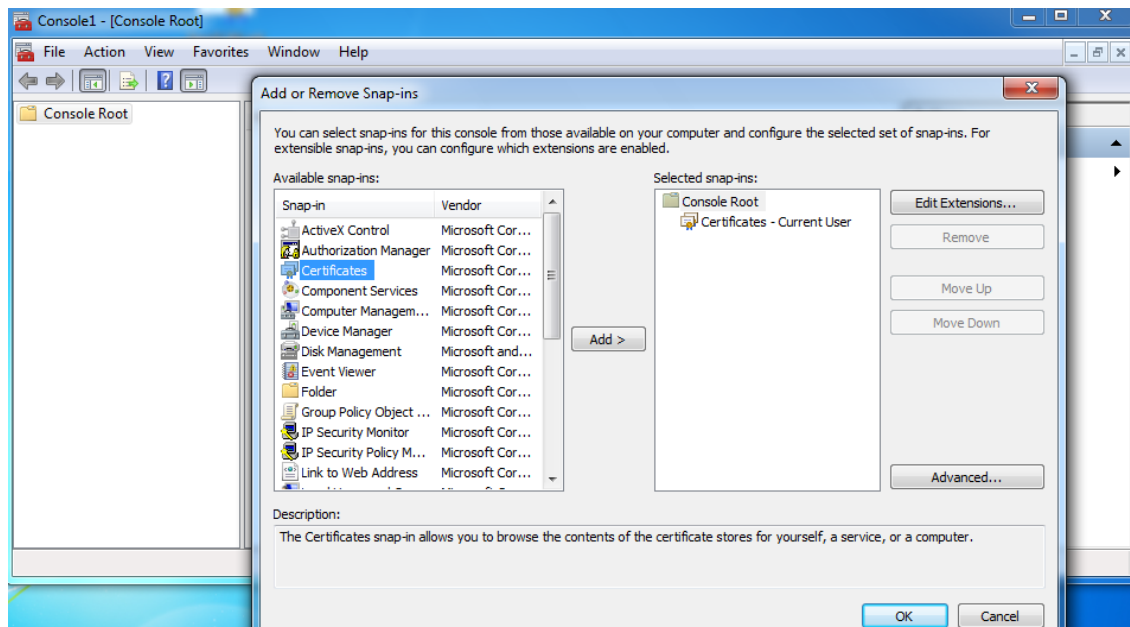
Ensure that the user certificate is being placed in the personal folder and click on **OK**.



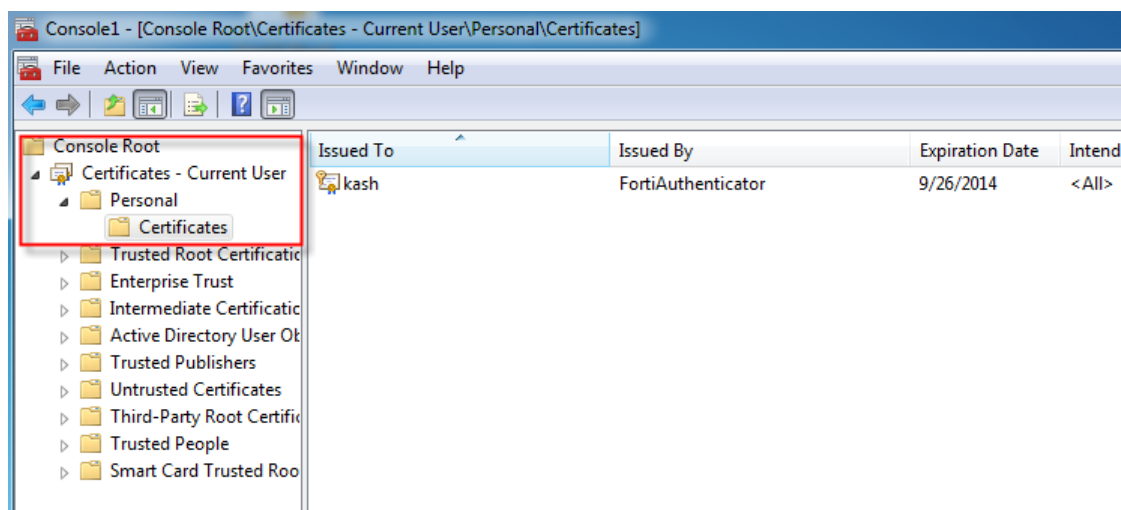
This should complete the user certificate import process and the following prompt should appear.



However, it is important to ensure that the certificate has been imported correctly and into the appropriate certificate store. To confirm the procedure, click on the windows icon and type mmc, then press enter. Then click on *File > Add/Remove Snap-In* and select the *Certificates snap-in*, as shown below, then press **OK**.



In the certificate snap-in, open the personal certificate folder, this is where you should find the imported certificate. If this is not the case, do not proceed until the certificate is in place.



This completes the windows management console tasks, feel free to close the mmc or save the view, it is no longer required in this setup. The certificate tasks on the FortiAuthenticator are now also complete.

FortiAuthenticator Directory Services Configuration

The following section covers FortiAuthenticator directory integration. To configure integration with a remote AD/LDAP, within the user interface, under *Authentication>Remote Auth. Servers>LDAP*, click on **Create New**, then complete the AD server settings in format similar the output below.

Name:	server-2008		
Server name/IP:	10.1.2.122	Port:	389
Base distinguished name:	dc=fortiad,dc=net		
Bind type:	<input type="radio"/> Simple <input checked="" type="radio"/> Regular		
Username:	cn=admin,dc=fortiad,dc=net	Password:
User object class:	person		
Username attribute:	sAMAccountName		
Group membership attribute:	memberOf		
Secure Connection			
<input type="checkbox"/> Enable			
Windows Active Directory Domain Authentication			
<input checked="" type="checkbox"/> Enable			
Kerberos realm name:	FORTIAD.NET		
Domain NetBIOS name:	SERVER		
FortiAuthenticator NetBIOS name:	FAC_v3b1		
Administrator username:	administrator		
Administrator password:		

The username and password required does not necessarily have to be an administrator; the user only requires enough rights to browse the directory for the purposes of pulling users and groups into the FortiAuthenticator.

<div><div>Delete</div><div>Import</div><div>View Certificate Detail</div><div>Download</div></div>			
<div></div>	<div>Name</div>	<div>Subject</div>	<div>Ref.</div>
<div></div>	CA_Cert_1	CN = FortiAuthenticator	<div>0</div>
<div></div>	Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com	<div>0</div>
<div></div>	PositiveSSL_CA	C = GB, ST = Greater Manchester, L = Salford, O = Comodo CA Limited, CN = PositiveSSL CA	<div>0</div>

FortiGate RADIUS Client Configuration

The FortiGate now needs to be configured as a RADIUS client to the FortiAuthenticator. Within the FortiGate interface, go to *User & Device > Authentication > RADIUS Server* and click on **Create New**. Complete the RADIUS server details, and then **test** the connection, example below.

Next, a wildcard RADIUS user needs to be created. Go to *User & Device>User>User Definition* and click on **Create New**. Then create a wildcard user as shown below. A wildcard user will allow the FortiGate to send all RADIUS authentication requests to the FortiAuthenticator.

The next RADIUS configuration step is to create the RADIUS group on the FortiGate which will be host the user(s) for the SSL-VPN. Within the FortiGate interface go to *User & Device > User*

> *User Group* and click on **Create New** and create a firewall authentication group that includes the wildcard user and references the FortiAuthenticator, example below.

Edit User Group

Name: radius-auth

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members: *

Remote authentication servers

Remote Server	Group Name
FortiAuth-Radius-29	Any

OK Cancel

Then go back to the wildcard card user, *User & Device>User>User Definition* and add the wildcard user to the RADIUS group and **OK** the changes, example below.

☒ Add this user to groups

- ☐ Guest-group
- ☐ dummy-redirect
- ☐ fortiad_net-group
- ☐ radius
- ☒ radius-auth

FortiGate SSL-VPN Configuration

The following steps address SSL-VPN creation on the FortiGate. Firstly ensure that there is a valid IP pool in place (under *Firewall Objects > Addresses*), if using an IP tunnel based VPN. To begin the SSL configuration, for both IP tunnel based and browser only VPN, go to *VPN > SSL > Config* and ensuring the relevant settings are in place and that the 'Require Client Certificate' tickbox is selected, as in the example below.

SSL-VPN Settings

IP Pools: SSL_RANGE_10_1_2_X, SSLVPN_TUNNEL_ADDR1

Server Certificate: Self-Signed

Require Client Certificate ☒

Encryption Key Algorithm: ☒ Default - RC4(128 bits) and higher

Idle Timeout: 300 (seconds)

Login Port: 10443

☐ Allow Endpoint Registration (Tunnel Mode Only)

Advanced (DNS and WINS Servers)

Apply

Then under *VPN > SSL > Portal* create the relevant SSL portal interface based on your VPN type (either *IP tunnel* or *browser only*), IP tunnel based VPN is shown in the example below.

Within the FortiGate interface, go to *Policy > Policy* click on **Create New**, then click on VPN setup and create an external interface to internal interface SSL-VPN policy, ensuring that you enable the ‘SSL client restrictive tickbox’ as shown in the example below.

From within the policy configuration click on **Create New** under the ‘*Configure SSL-VPN Authentication Rules*’ section and use the preconfigured RADIUS group and the SSL-VPN portal as in the example below, **OK** the changes and then **OK** the main policy.

New SSL VPN Authentication Rule

Group(s)

radius-auth

User(s)

Click to add...

Schedule

always

SSL-VPN Portal

tunnel-access

Action

ACCEPT

Logging Options

No Log

Log Security Events

Log all Sessions

Security Profiles

OFF AntiVirus

default

OFF Web Filter

default

OFF Application Control

default

OFF IPS

default

OK

Cancel

If the completed SSL policy is selected and **edited**, the configuration should be as follows.

New Policy

Policy Type

Firewall VPN

Incoming Interface

port2 (external)

Remote Address

all

Local Interface

port1 (internal)

Local Protected Subnet

webserver [10.1.2.31]

SSL Client Certificate Restrictive

Cipher Strength

Any

Configure SSL-VPN Authentication Rules

Create New

SSL

Delete

User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
radius-auth	ALL	always	-	tunnel-access		ACCEPT
ANY	ALL	always	-			DENY

Comments

Write a comment...

0/1023

OK

Cancel

When configuring an IP tunnel SSL-VPN (using the FortiClient), then an additional firewall policy is required (configured *Policy > Policy* and then **Create New**), this is to allow incoming connections from the SSL tunnel interface to the internal network. An example of this is as follows.

New Policy

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	ssl.root (sslvpn tunnel interface) +
Source Address	SSL_RANGE_10_1_2_X +
Outgoing Interface	port1 (internal) +
Destination Address	webserver [10.1.2.31] +
Schedule	always v
Service	ALL +
Action	✓ ACCEPT v
<input type="checkbox"/> Enable NAT	
Logging Options	
<input type="radio"/> No Log	
<input checked="" type="radio"/> Log Security Events	
<input type="radio"/> Log all Sessions	

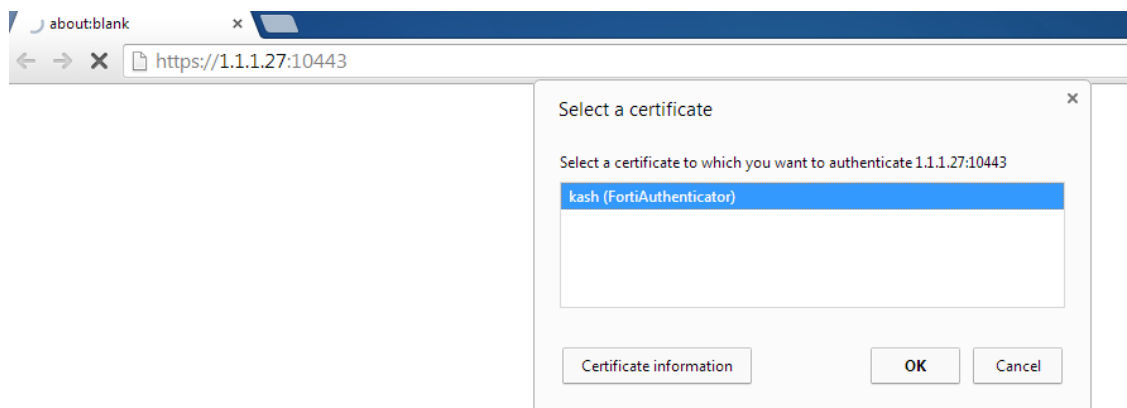
Once you **OK** the changes, the completed rule should look as follows in the policy section.

▼ ssl.root (sslvpn tunnel interface) - port1 (internal) (2 - 2)						
2	SSL_RANGE_10_1_2_X	webserver [10.1.2.31]	always	ALL		✓ Accept

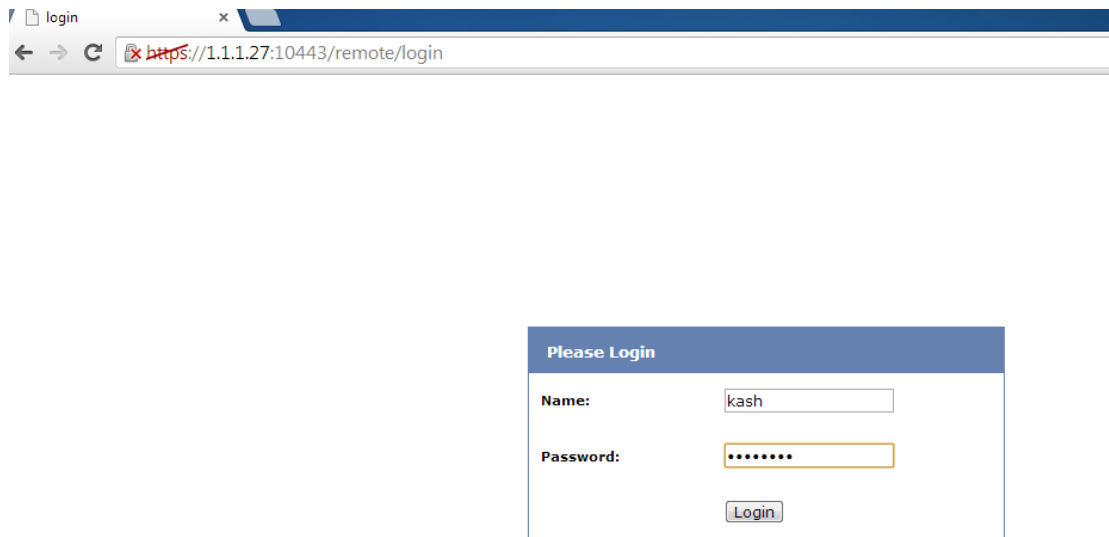
This completes the all configuration steps. It is now time to test the VPN.

Testing, Logging and Monitoring

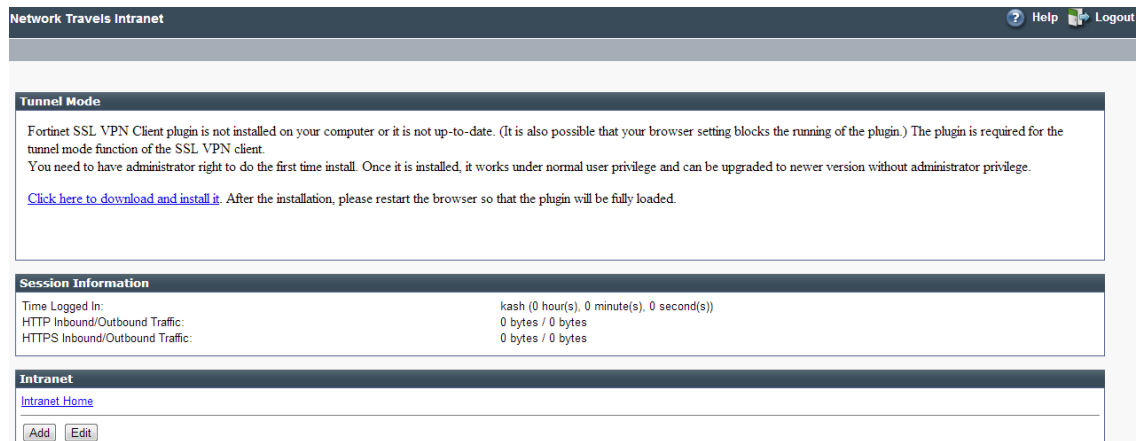
If the configuration is for a browser only SSL-VPN, then open a browser to the SSL-VPN gateway. Upon connecting to the gateway, the certificate negotiations should begin and the browser should prompt for a valid user certificate to be used for the VPN, any certificates in the personal certificate store will be listed. See example below using the Chrome browser.



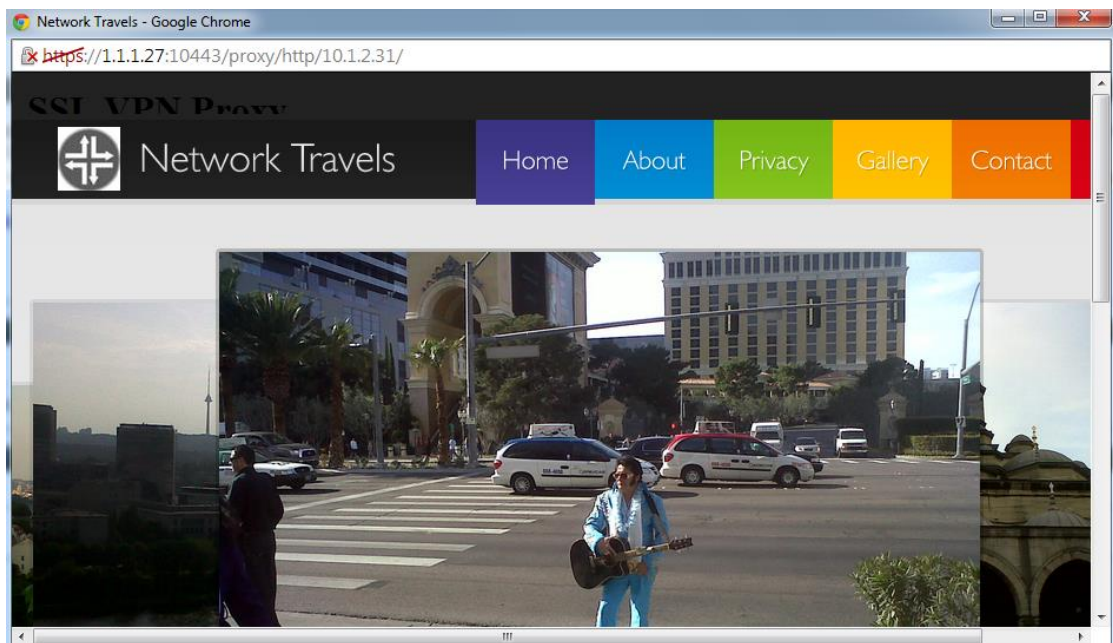
Upon successful certificate negotiations, a username and password prompt should appear. Even if the certificate negotiations fail, the username and password prompt will still appear, however it will not be possible to successfully authenticate, even if the username and password are valid.



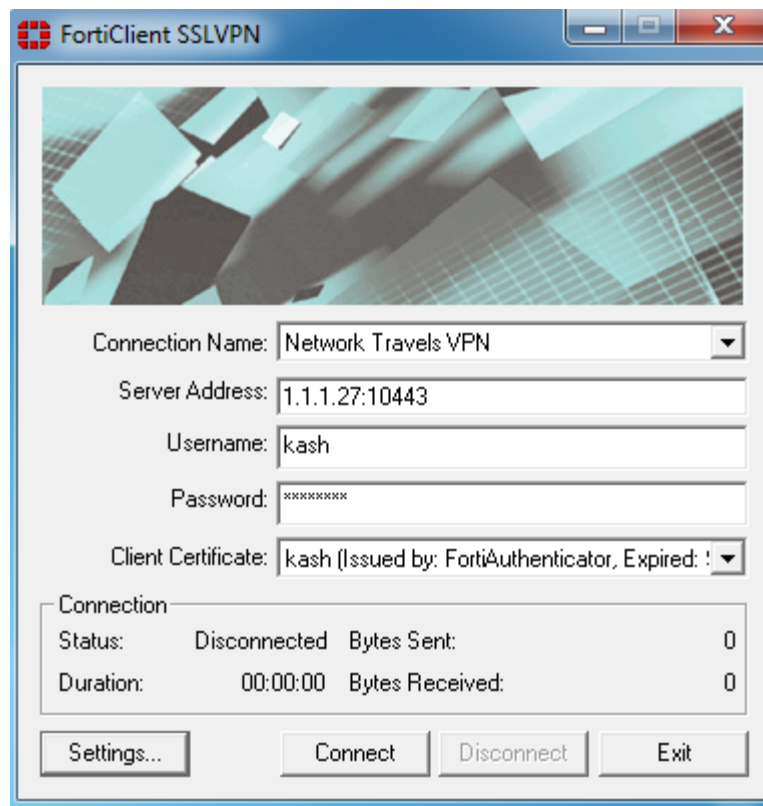
Once the current directory username and password have been entered, then the SSL-VPN portal should be available, example below is of the portal configured earlier in this guide.



On clicking on the 'Intranet Home' page, the browser connection is then proxied to the internal web server, example below.



If the configuration is based on an IP tunnel configuration, then the FortiClient is required to initiate the connection. The FortiClient should automatically pull the personal certificate from the local certificate store and make it available in the connection settings. See example below.



Click on *Connect* to initiate the VPN and certificate negotiations, if the certificate negotiations fail, there should be an '-12 error message' prompt and the VPN will not complete. If the certificate settings are valid and the directory username and password is correct, the VPN should connect and data transfer should begin. To confirm that the client is connected, **click**

on the windows icon and enter 'ipconfig', the fortissl adapter should be visible with the correct preconfigured address.

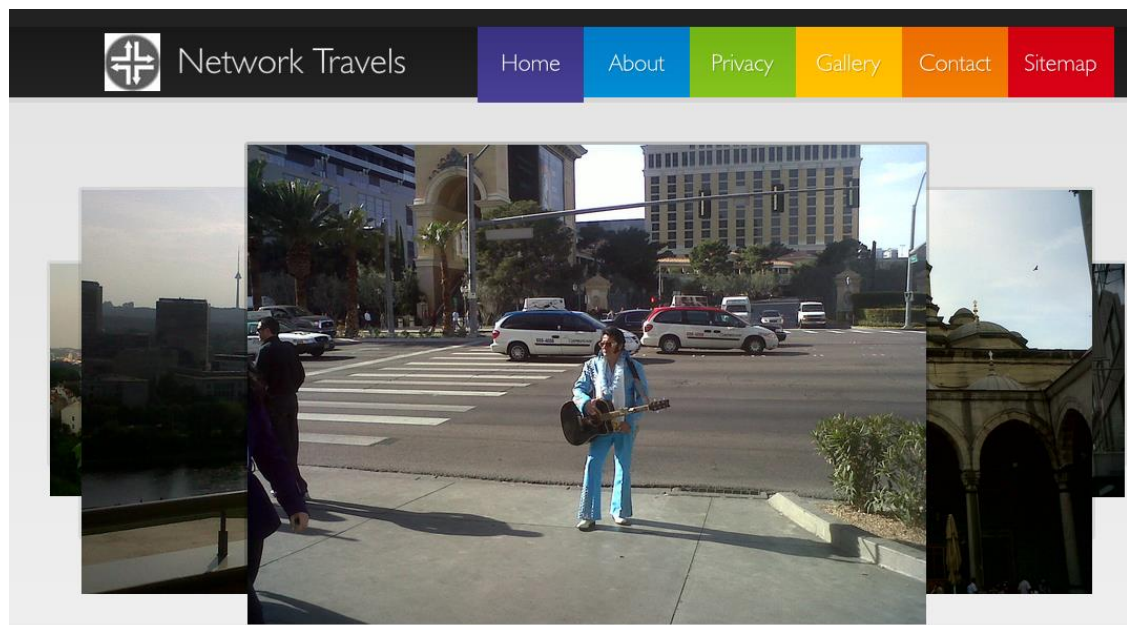
```
C:\Users\kash>ipconfig

Windows IP Configuration

PPP adapter fortissl:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.1.2.151
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . :
```

The client PC should be able to connect to the internal network directly; the snapshot below is of the client browser connecting directly (via the 10.1.2.31 address) to the intranet.



Recent Updates

Aggregating IP Flows

If logging had been enabled on the relevant FortiGate firewall policies, these should also be incrementing their counters and indicating data transfer.

Within the FortiGate interface, under *VPN > Monitor > SSL-VPN Monitor*, the monitor status should indicate that the client is connected. In the example below, the tunnel IP is also shown as this is a IP tunnel based VPN.

	No.	User	Source IP	Begin Time	Description
<input type="checkbox"/>	1	kash	1.1.1.1	Fri Sep 27 08:50:12 2013	
<input type="checkbox"/>			Subsession		Tunnel IP:10.1.2.151

Within the FortiAuthenticator interface, under *Logging > Log Access > Logs* the following entry confirms that the user has successfully authenticated against Active Directory.

386	Fri Sep 27 08:49:49 2013	information	Event	Authentication	20001	10.1.2.27	Remote LDAP user authentication with no token successful	kash
-----	--------------------------	-------------	-------	----------------	-------	-----------	--	------

This completes and confirms the SSL-VPN client testing.

Additional Considerations - Certificate Checking

With the above setup, the FortiGate does not check the validity of the received client certificate. This can be achieved through the use of a CRL (Certificate Revocation List) and CDP (CRL Distribution Point). The CRL is a list of certificates the FortiAuthenticator has revoked, and is available to download as a static list. The CDP is in every certificate the FortiAuthenticator issues and provides a link for the CRL. OCSP (Online Certificate Status Protocol) is a real-time certificate check with the Certificate Authority. Upon receipt of a certificate, a device can check the validity of the certificate from the issuing authority by using OCSP. FortiAuthenticator supports CRLs, CDPs and OCSP.

The dynamic OCSP CRL is accessible via the URL:

http://<FortiAuthenticator_IP>:2560

Added Benefits

- FortiAuthenticator can introduce Certificate Management to an existing FortiGate install base with minimal disruption
 - With an easy to use interface and rich feature set, customers can increase the security of existing SSL or IPSec VPNs
- FortiAuthenticator supports SCEP (Simple Certificate Enrolment Protocol), which means users can generate and auto-enroll their certificates, rather than manually creating them
- Very useful in BYOD and smartphone/tablet scenario's
- FortiAuthenticator can import users from an existing directory server and associate multiple authentication methods to the user such as FortiTokens, SMS and E-mail
- Users and Groups can be auto-imported (based on rules) from the directory server
- Active Directory authenticated users can feed into the FSSO (Fortinet Single Sign-On) framework allowing Identity Based access control across the network

